ABSTRACT

A protocol designing method that securely performs a password-based authentication and key exchange protocol using a zero-knowledge interactive proof is disclosed. According to this method, various kinds of system parameters required for authentication are first set. Then, a user selects a certain random number in conformity with the set parameters, and sends to a server a message including a user ID, a test number A applying a one-way function, and a first question number generation value X known only to the server and the user. The server, using the message sent from the user, sends to the user a message including an authentication Auth of whether the server possesses a public key, and a second question number generation value Y known only to the server and the user. The user authenticates the server by verifying the authentication Auth, and computes a resultant value c of a secret coin tossing known only to the server and the user and a session key SK. Thereafter, the user sends to the server a witness number B for user authentication. The server that stores a password verifier V for the respective user verifies the witness number B using the value c, and exchanges the session key SK by computing the session key SK. Accordingly, a secure authentication and key exchange can be performed only using the password without the necessity of any tool such as a smart card.